Home vs. Enterprise wireless networks

Nicolas Janis

Independence High School

ENG 111

Mr. Palmer

January 15, 2022

Home vs. Enterprise wireless networks

Millions of packets whizzing by invisible to those around. The very lifeblood of the coveted resource many know as the internet. This resource, also known as WiFi, is the wireless connection that many uses to connect to the internet. Most love it when it is working, while everyone panics when it stops working. This had led to many claiming that their WiFi networks are home are that much better than those in schools and other enterprise environments. However, as home networks, truly that much better and more reliable than the school/enterprise networks at a base level?

IEEE 802.11 Standard

The Institute of Electrical and Electronics Engineers (IEEE) standard 802.11, also more commonly known as WiFi is the set of defining rules that govern WiFi and how it works. WiFi itself is simply a set of broadcast radio signals that devices such as phones, tablets, smart-watches, etc. understand as WiFi or the method they use to wirelessly reach out to the internet. So what separates the WiFi in the average household from that found in schools? Simply put, it is the objects surrounding the wireless network and how it is constructed that truly separate these various networks apart. The first outstanding factor that can make a difference in the overall effectiveness of one's wireless network is the version of WiFi or 802.11 standards that they are using. The 802.11 standards are separated into various versions with the main difference between them being improvements from the last standard, in theory making them better. These standards comprise 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax. There are three main differences between these wireless standards and that comes down to the frequency they use, the bandwidth they are capable of, and their effective distance. For example, 802.11g is broadcasted at 2.4 GHz (gigahertz), is capable of speeds up to 54Mbps (megabits per second), and has an effective distance of up to 150 feet. (Hardwood, 2009) This in contrast with the 802.11n which is broadcasted at 2.4 and 5.0 GHz, is capable of speeds up to 600Mbps and has an effective distance of up to 175 feet or more. (Hardwood, 2009) From this we can begin to see the difference in the

standards and why different standards are better than others. However, what is 2.4 GHz and 5.0 GHz and why is it important?

2.4 GHz and 5.0 GHz are the radio frequencies that have been defined by the 802.11 standards as that used for wireless. They are important, not only because they are the frequencies that are used, but also because they contain some key differences that can affect performance in certain cases. This comes down to the physics of radio signals and how "big" these frequencies are. This size difference in the two frequencies means that 5.0GHz can carry more data at any given time, however, the physics of this radio signal means that it cannot go through objects just as walls as well, compared to the "smaller" 2.4GHz signal. In others words, 2.4GHz signals cannot carry as much data as their 5.0GHz counterparts, however, they can often travel further distances indoors as their signal does not degrade as much through various building materials.

The fact that WiFi is simple a set of broadcast radio signals the physics of these signals can create various issues that can affect the overall performance of the wireless network. As stated before building materials can affect the strength of the signal, however, three other factors can heavily impact the effectiveness of the wireless network. These factors include Electromagnetic Interference (EMI), Radio Frequency Interference (RFI), and channel overlap. EMI and RFI are simply interference created by competing signals whether that be the electromagnetic fields created by nearby electronic devices or other wireless signals. For example, if you have ever taken two hand-held radios and pushed the push-to-talk button at the same time you simply get static. The same concept is true for WiFi, if WiFi signals are broadcasted near each other they have the ability to overlap and cancel each other out, in short canceling out the signal directly affecting the wireless network. This is where channel overlap comes into play, the 2.4GHz and 5.0GHz frequencies are divided up into various channels, a kind of barrier to divide up the frequency spectrum. If two nearby wireless networks are on the same channel or neighboring channels this can create RFI directly affecting the effectiveness of the wireless network.

Network Construction

When comparing wireless networks they can often be separated into two categories, home networks, and enterprise networks. The difference often comes down to the equipment used and their overall construction. For example, home networks often use an all-in-one router compared to enterprise networks that will often use a separate router and wireless access points (WAPs). This is important because these all-in-one routers are often poorly designed and do the job of a router, WAP, firewall, and more. This causes issues in that router gets overloaded and this also causes the router to not perform any of these jobs particularly well, however, one box is easier to manage than multiple. However, this is not the only design choice that often causes issues in a home network. One design choice that often causes issues in home networks is the placement of this router. As stated before, the more walls and materials that the wireless signal has to travel through the weaker it becomes. This is why devices often have weaker signals the further away they get from the router and since the router is the only source of the wireless signal in a home network this causes issues. This is directly compared to the use of WAPs in an enterprise network. These are small devices that broadcast their own wireless signal, this allows you to have the equivalent of multiple home routers. This helps to fix the issue of the signal degrading over distance, however, introduces a new issue. Similar to the channel issues discussed before, if you put two WAPs to close together you get the same issue. Another, design choice that often differs between home networks and enterprise networks is the underlying wired side of the network. Home networks often use mesh systems, meaning that the various network devices are wirelessly connected. This is directly compared to enterprise networks where most of the underlying infrastructure running the wireless is wired together. This practice of mainly using a wired underlying infrastructure, while more tedious to upkeep has the added benefit of having fewer issues when compared to a mesh system. This reliability in an enterprise environment means that in normal conditions the enterprise network is more likely to stay up and operational compared to a home network. This comes down to the fact enterprise networks are designed with three factors in mind these are reliability, ease of use, and availability. (Murty et al., 2008) This is directly

compared to home networks that often only focus on ease of use and do not put as much weight on reliability and availability.

Even with all this considered the part where enterprise networks often fall short, such as in schools like LCPS, is the number of devices that are trying to connect to the network at any given time. As discussed before, the more devices you have on a network at any given time the worse the network tends to perform. This was directly tested in Sundaresan, Feamster, and Teixeira's paper Measuring the performance of user traffic in-home wireless networks. As the number of users went up in the network the total throughput to any given device was lowered, with 5.0GHz networks performing better. (Sundaresan et al., 2015) This is only further amplified in enterprise networks where a network is going from seeing less than 10 or 20 devices, compared to a network such as LCPS' seeing a couple thousand at any given time. This increase of users makes the network appear to perform worse when if the networks themselves were compared head to head under ideal conditions the enterprise network would prevail.

Conclusion

As seen throughout this paper, enterprise networks such as LCPS, seem to appear to perform worse compared to home networks. These issues that both have and the gaps that networks such as LCPS have to overcome in order to have a working WiFi outperform home networks by a large margin. The misconception that home networks are built better and therefore perform better is merely a myth. The fact that enterprise networks need to be built to handle a large volume of clients at any given time, means that in a head-to-head comparison with the same conditions the enterprise network would outperform the home network. The fact that enterprise networks have to deal with larger volumes of clients as well as other issues created by security policies not discussed in this paper, that home networks do not have to deal with means that home networks appear to perform better. This is not to say that either network cannot be improved, at a surface level home wireless networks compared to their enterprise counterparts, the enterprise network outperforms the home wireless network. In short, when compared head to head, the fact

the home networks a designed and perform better than enterprise networks such as LCPS is simply a myth, and when the pure data is compared enterprise networks come out on top.

References

Hardwood, M. (2009). Pearson it certification. https://www.pearsonitcertification.com/articles/article.aspx?p=1329709&seqNum=4

Jain, R. (2016). Ieee 802.11 wireless lans part i: Basics. https://www.cse.wustl.edu/~jain/cse574-16/ftp/j_05lan.pdf

Murty, R., Padhye, J., Chandra, R., Wolman, A., & Zill, B. (2008). Designing high performance enterprise wi-fi networks. *NSDI*, *8*, 73–88.

Sundaresan, S., Feamster, N., & Teixeira, R. (2015). Measuring the performance of user traffic in home wireless networks. *International Conference on Passive and Active Network Measurement*, 305–317.